UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/692,709	10/19/2000	Christian Gehrmann	45687-00036	7545

38065 7590 04/28/2005

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR C11
PLANO, TX 75024

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 04/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/692,709	**Applicant(s)** GEHRMANN ET AL.	
	Examiner Brandon Hoffman	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 4-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 4-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 and 4-23 are pending in this office action. Claim 3 having been cancelled.

Rejections

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

3. Claims 1 and 4-6, 17, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merging and Extending the PGP and PEM Trust Models – The ICE-TEL Trust Model, Chadwick et al., May/June 1997 (hereinafter referred to as Chadwick et al.).

Regarding claims 1, 4, 5, and 17, Chadwick et al. teaches a method/ad hoc communication network for establishing security in an ad hoc communication network, the ad hoc communication network comprising:

- A set of communication nodes (fig. 2, pg. 20),
- At least two nodes of the set of communication nodes having a mutual trust relation and comprising a trust group (pg. 20, right column, first full paragraph),

  - The trust relations being created with public keys, and at least one additional node (fig. 4, pg. 22),
    - The at least one additional node being a candidate node for joining the trust group within the ad hoc communication network (pg. 22, left column, first paragraph),
- The nodes having authority to delegate trust to nodes of the set of communication nodes within the trust group (pg. 20, "Certification Path"),
- The method comprising the steps of:
  - Receiving a request from the candidate node to join the trust group within said ad hoc communication network wherein said ad hoc communication network does not include a separate certificate authority (pg. 20, left column, last paragraph. Chadwick teaches (page 19, "Trusted Point") that a security domain can be as small as a single user with a user as its trusted point, not a certificate authority.); and
  - Identifying a node of the set of communication nodes within the trust group having a trust relation with the candidate node (pg. 20, right column, "Cross Certification"), the node having the trust relation with the candidate node being an X-node, **and**
  - **Wherein X-node further sending a signed message comprising a list of nodes that the X-node trusts within the ad hoc communication network and all corresponding public keys to the candidate node** (pg. 20, left column, first paragraph).

Chadwick et al. does not specifically teach distributing trust relations between all members in the trust group and the candidate node by means of the X-node distributing the public key associated with said candidate node to said all members of the trust group. However, Chadwick et al. teaches distributing the public keys and trust relations between all members in the trust group and the candidate node, but is silent on the exact steps involved in distributing (pg. 19, right column, last paragraph).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the X-node distributing the public key of the candidate node to all members of the trusted group, with the method/network of Chadwick et al. It would have been obvious for such modifications because in the public-key cryptographic system of Chadwick et al. (a system where each device holds secret its private key and allows its public key to be freely distributed), distributing your public key to all the devices/users that you want to be able to communicate with securely, allows the devices/users to encrypt communications with your public key so that only you can decrypt the communications with your secretly held private key. This is desirable because in a wireless ad hoc network, where devices have no base stations or agreed upon topology, a device has the ability to broadcast/publish its public key for any device/user willing to communicate securely with the device.

[Terms in parentheses correspond to the claimed limitations of the instant application]

Imagine an example where there are people at a party (ad hoc network). Everyone (nodes that are already members of the network) already knows each other at the party. The host (X-node) of the party invites a friend (candidate node) to come over that no one knows, except for the host who invited the friend. The friend doesn't know anyone at the party either, except for the host. It is the host's job to tell everyone already at the party the friend's name (X-node distributes the public key of the candidate node to the other members of the ad hoc network). It is also the host's job to tell the friend everyone else's name that are already at the party (this is the signed message with public keys of the members. It is signed because the friend trusts the host of the party). This way, each person has a mental list (a table of public keys of the ad hoc network) of every other person's name at the party. The people at the party are allowed to move freely about the party (perhaps changing the network topology of the ad hoc network).

Regarding claims 6 and 18, Chadwick et al. teaches wherein the ad hoc communication network comprises a set of nodes comprising several trust groups (fig. 4, pg. 22), each of the set of nodes being candidates for joining all trust groups within the ad hoc communication network that the set of nodes are not already a member of (pg. 22, left column, second paragraph), the method comprising, after receiving the messages, each node of the set of nodes creating a list of candidate nodes that a given node of the set of nodes trusts and corresponding public keys (pg. 22, left column, first paragraph).

Claims 7-16 and 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chadwick et al. in view of Morris et al. (U.S. Patent No. 6,691,173).

Regarding claims 7 and 19, Chadwick et al. teaches all the limitations of claims 1, 6 and 17, respectively, above. However, Chadwick et al. does not teach deciding one node within the ad hoc communication network to act as a server node.

Morris et al. teaches further comprising deciding one node within the ad hoc communication network to act as a server node (col. 4, lines 49-56).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine deciding one node to act as a server node, as taught by Morris et al., with the method/network of Chadwick et al. It would have been obvious for such modifications because an ad hoc network needs to establish one node as the server, while the other nodes act as slaves. This step is necessary and is therefore a desirable and obvious step.

Regarding claim 8, the combination of Chadwick et al. in view of Morris et al. teaches further comprising the server node receiving, from each other node within the ad hoc communication network, a message comprising a respective public key, a respective list of candidate nodes that the respective node trusts, and corresponding public keys (see col. 3, line 49 through col. 4, line 2 of Morris et al.).

Regarding claims 9 and 20, the combination of Chadwick et al. in view of Morris et al. teaches further comprising the server node classifying the at least one candidate node as being a server-trusted node or as being a server-untrusted node, depending on whether the server node trusts the at least one candidate node or not (see pg. 22, left column, second paragraph of Chadwick et al.).

Regarding claims 10 and 21, the combination of Chadwick et al. in view of Morris et al. teaches wherein the identifying step further comprises the server node identifying at least one Y-node required for distributing trust relations between the server node and at least one server-untrusted node (see col. 8, lines 23-37 of Morris et al.).

Regarding claims 11 and 22, the combination of Chadwick et al. in view of Morris et al. teaches wherein said distributing step further comprises sending, by the server node, of a request to the identified at least one Y-node to distribute said trust relations between the server node and the server-untrusted nodes (see col. 8, lines 38-45 of Morris et al.).

Regarding claim 12, the combination of Chadwick et al. in view of Morris et al. teaches wherein said distributing step further comprises obtaining, by the server node, of said requested trust relations (see col. 8, lines 45-49 of Morris et al.).

Regarding claim 13, the combination of Chadwick et al. in view of Morris et al. teaches wherein the step of obtaining the trust relations further comprises:

- Signing, by the Y-node, of the public key of the server node for each server-untrusted node that the Y-node has a trust relation with (see pg. 20, "Certification Path" of Chadwick et al.); and
- Forwarding, by the Y-node, of said signed public key to the server-untrusted node (see pg. 20, "Certification Path" of Chadwick et al.).

Regarding claim 14, the combination of Chadwick et al. in view of Morris et al. teaches wherein the step of obtaining the trust relations comprises:

- Signing, by the Y-node, of the public key of the server-untrusted node for each server-untrusted node that the Y-node has a trust relation with (see pg. 20, "Certification Path" of Chadwick et al.); and
- Forwarding, by the Y-node, of said signed public key to the server node (see pg. 20, "Certification Path" of Chadwick et al.).

Regarding claim 15, the combination of Chadwick et al. in view of Morris et al. teaches comprising the further step of, after obtaining said trust relation, reclassifying, by the server node, the server-untrusted node with the obtained trust relation as being a server-trusted node (see col. 8, lines 45-49 of Morris et al.).

Regarding claims 16 and 23, the combination of Chadwick et al. in view of Morris et al. teaches comprising the further step of sending, by the server node, of a signed message comprising the server node's trusted public keys belonging to trusted candidate nodes within the ad hoc communication network (see col. 4, lines 3-8 of Morris et al. and pg. 20, right column, "Cross Certification" of Chadwick et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoff

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 21